MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2016/2017

TMI 3231 – MALWARE AND INTRUSION DETECTION

(All sections / Groups)

24 FEBRUARY 2017
3.00 p.m – 5.00 p.m
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 5 pages with 6 Questions only.
2. Attempt **ALL SIX** questions. All questions carry equal marks and the distribution of the marks for each question is given.
3. Please print all your answers in the Answer Booklet provided.

QUESTION 1

a) The terms "Attack" and "Vulnerability" are commonly used across the security sector. Demonstrate your understanding by explaining these two terms and provide any FOUR (4) types of attacks.

(4 marks)

b) McCumber Cube is a 3x3x3 cube representing the various areas that must be addressed to secure today's information systems. List any SIX (6) areas that have been covered by McCumber Cube.

(3 marks)

c) A furniture shop has launched its new website which is meant for customers to order the custom-made furniture. However, since the launch of the new website, the shop is faced with a sudden increase of attacks and issues. After a thorough inspection, you have identified that the problem is due to the password management that are incorporated in the new website. Now that you know the cause, list THREE (3) potential attacks/issues related to password management of the website.

(3 marks)

QUESTION 2

a) You suspected that the files in your company's computer system have been infected by the virus. After inspection, the files are infected by two types of viruses, which are overwriting viruses and cavity viruses. In order to log a detailed report to your manager, explain how these viruses work to infect the files.

(2 marks)

b) There are four generations of anti-virus software inclusive are first generation (simple scanners), second generation (heuristic scanners), third generation (activity traps) and fourth generation (full featured protection). Discover the differences among each of them.

(4 marks)

c) Phishing, Vishing and Pharming are the popular tactics of social engineering. Each method has its own distinguishing characteristics. But they all have the same goal. Identify their similar goal and dissimilar characteristics.

(4 marks)

Continued...

QUESTION 3

a) As a security expertise, you will have to understand the common security tasks a firewall provides. Identify any FOUR (4) firewall security tasks.

(4 marks)

b) Your company would like to purchase a new firewall system and you think that the application layer gateways seem to be suitable for your company. Justify how application layer gateways work and how they can help to protect your company's network.

(4 marks)

c) Bob would like to purchase a stateful packet filter to protect his home network. However, he was told that stateful packet filter have some well-documented limitations. Briefly explain these limitations.

(2 marks)

QUESTION 4

a) You are asked to setup with a screened-host system and you understand that the screened-host firewall is a more flexible firewall than the dual-homed host firewall. Discuss how the flexibility and the security can be achieved by the screened-host firewall.

(3 marks)

b) Remote Management Interface is a software used to configure and monitor one or more firewalls that are located at different network locations. Based on your opinion, what are the benefits can be offered through the remote management interface if you have three firewalls planted on each endpoint of your network?

(3 marks)

c) ABC Company would like to purchase a machine and configure it as a bastion host to serve as its company's web server.

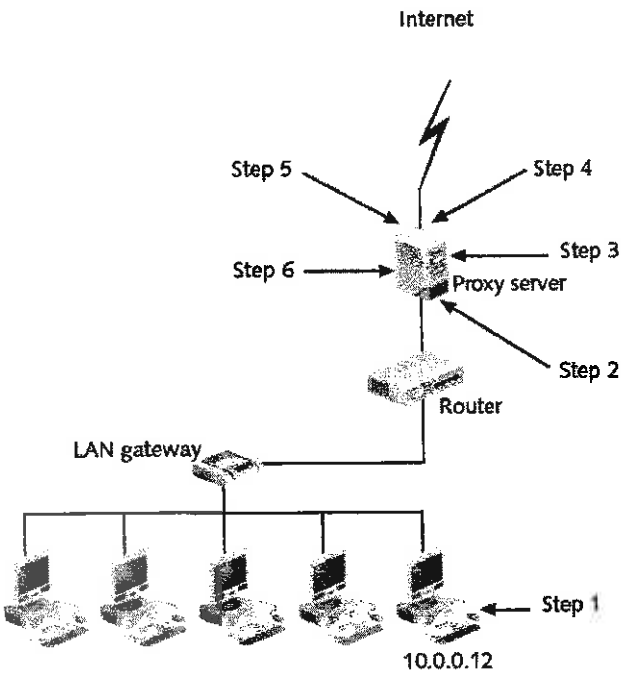
i. What is the reason for running the web server on a bastion host?
ii. Elaborate THREE (3) important steps to secure a bastion host.

(4 marks)

Continued...

QUESTION 5

a) There are several steps involved in a proxy transaction. Assume that a request is sent from the internet (Step 1) to the proxy server (Step 2) as illustrated in the figure below, explain the rest of the steps (Step 3 – 6) taken by the proxy server to establish the connection between the local host and an external host.



(4 marks)

b) Some organizations set up the Honeypot server to make the host defend itself. What do you know about Honeypot server? Why do some security professionals advise against using Honeypots?

(3 marks)

c) Nowadays we rely on Bluetooth networks to connect our mobile device to headphones, speakers, and other devices, but there are security concerns surrounding bluejacking and bluesnarfing. Differentiate between bluejacking and bluesnarfing.

(2 marks)

d) Bob cannot make his decision to apply MAC filtering on the network. What do you think is the main disadvantage of using MAC filtering?

(1 mark)

Continued...

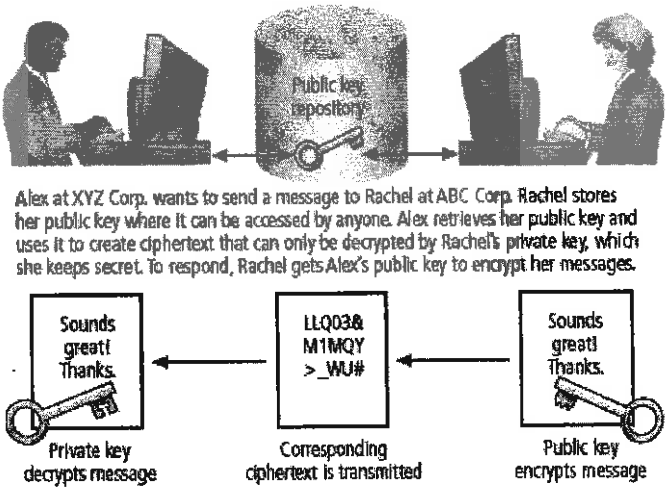
QUESTION 6

a) Bob obtained a message in cryptographic notation as below which he could not understand. He asked for your favor in translating the message. Could you explain the encryption process from the given message?

$$E(M, K) = C$$

(2 marks)

b) Given the figure below, name the encryption type and describe the encryption process that is implemented.


Public key repository
Alex at XYZ Corp. wants to send a message to Rachel at ABC Corp. Rachel stores her public key where it can be accessed by anyone. Alex retrieves her public key and uses it to create ciphertext that can only be decrypted by Rachel's private key, which she keeps secret. To respond, Rachel gets Alex's public key to encrypt her messages.
Sounds great! Thanks.
LLQ03& M1MQY >_WU#
Sounds great! Thanks.
Private key decrypts message
Corresponding ciphertext is transmitted
Public key encrypts message

(3 marks)

c) Your company has decided to connect its three branches via Virtual Private Network (VPN). Do you recommend your company to purchase three VPN concentrators to establish the connection? Justify your answer.

(2 marks)

d) As a security manager, you are to ensure that the operation of a Virtual Private Network (VPN) is successful. This depends not only on its hardware and software components and overall configuration but also on a number of best practices. What are the VPN best practices should be enforced here?

(3 marks)

End of Paper